Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection

Md Abdullahel Kafi[1*], Nazma Akter[2]

Graduate Research Assistant, Department of Decision and Information Sciences, Oakland University, **USA**
Assistant Professor, School of Business, Ahsanullah University of Science and Technology, Dhaka, **BANGLADESH**

*E-mail for correspondence: kafi6240@gmail.com

ABSTRACT

Securing financial information, especially accounting, is essential in the digital world. This article explores organizations' challenges in protecting accounting data from evolving cyber threats. By sharing real-life case studies and industry research, we offer suggestions to enhance the security of accounting information. These recommendations include adopting cybersecurity frameworks implementing technical defenses like endpoint protection and network segmentation, following secure coding practices prioritizing user awareness and training, creating incident response and business continuity plans, regularly conducting vulnerability assessments and monitoring, maintaining strong vendor relationships, and ensuring compliance with relevant regulations and standards. By implementing these suggestions, accounting professionals and organizations can strengthen cybersecurity measures. Effectively protect valuable financial data from the ever-growing threat landscape. Taking an approach that combines technical measures, user awareness, incident preparedness, and regulatory compliance is crucial when navigating the digital landscape with confidence and resilience.

Keywords: Accounting, Cyber-Security, Threats, Vulnerability

INTRODUCTION

The accounting industry has transformed due to the rapid advancements in technology. This has led to the digitization and automation of financial processes. However, with this digital revolution comes challenges and risks, particularly in protecting financial information (Gutlapalli, 2017). As accounting data increasingly exists, the importance of robust cybersecurity measures cannot be understated. In this article, we present a collection of real-life case studies that shed light on the significance of cybersecurity in safeguarding accounting data and mitigating risks.

Recent years have witnessed high-profile incidents that have exposed the vulnerabilities and potential consequences of inadequate data protection in the accounting sector. For example, the known Equifax data breach in 2017 resulted in the exposure of sensitive financial information belonging to millions of individuals. This incident caused financial and reputational damage to the company (Smith, 2017). Such instances highlight the need for accounting professionals to possess knowledge and expertise in cybersecurity practices to protect their client's financial information. The case studies included in this article provide real-world examples of cyber threats faced by accounting organizations. These studies explore types of attacks such as data breaches, ransomware incidents, and insider threats. By examining these cases, accounting professionals can gain insights into the methods employed by actors and understand the potential repercussions of compromised financial data.

Data breaches can have consequences, such as significant financial loss penalties from regulatory bodies and damage to the trust of customers (Ponemon Institute, 2020). On the hand, ransomware attacks can severely disrupt accounting operations and cause disruptions in service delivery and financial transactions (Jartelius, 2020). Insider threats though not as frequently discussed, can pose risks when employees unintentionally or deliberately mishandle or disclose sensitive financial information (Le & Zincir-Heywood, 2019). Accounting organizations must adopt cybersecurity practices to mitigate these risks. This article examines strategies and best practices that can strengthen data protection. It highlights the importance of implementing access controls, encryption techniques, and

network monitoring systems to detect and prevent unauthorized access.

Additionally, it emphasizes the need for employee awareness and training programs to cultivate a security-conscious culture within accounting firms. Accounting professionals and organizations can fortify their defenses by studying real-life case studies and implementing recommended cybersecurity measures. Reduce the chances of cyber-attacks. This article aims to raise awareness about the importance of cybersecurity in the accounting sector while equipping professionals with insights and recommendations for effectively safeguarding sensitive financial information. The increasing digitalization of accounting processes necessitates a focus on cybersecurity.

The case studies discussed in this article serve as reminders about the potential dangers that accounting organizations face and the severe outcomes that result from insufficient data protection. By implementing cybersecurity measures, accounting professionals can protect financial information, maintain their client's trust, and preserve the integrity of the accounting profession in the digital age.

Methodology

In this article, we employ a research method that examines real-life examples to shed light on the cybersecurity issues surrounding safeguarding financial information in the digital world. The author has gathered data from trusted sources and analyzed it to uncover patterns, weaknesses, and the impact of protecting accounting data. Using our analysis as a foundation, we have formulated practices and suggestions. Combining our case studies' findings with these recommendations, the article offers insights and practical advice for accounting professionals and organizations aiming to strengthen their cybersecurity measures.

Literature Review

The accounting field has been receiving increased attention when it comes to cybersecurity. As financial processes become more digitized, the risk of data breaches and cyber-attacks becomes more prominent (Kafi & Adnan, 2020). This review explores the existing research and scholarly contributions that discuss ways to secure information in the digital world. The study hopes to gain insights into the challenges faced and the best practices in cybersecurity for protecting accounting data.

In the accounting industry, data breaches have become a cybersecurity threat. A report called the "Cost of a Data Breach Report" by the Ponemon Institute has played a role in quantifying the financial implications of such breaches. It highlights the average cost per compromised record, legal expenses, and customer churn rates (Ponemon Institute, 2020). These findings emphasize the need for robust cybersecurity measures to prevent and mitigate the financial consequences of data breaches.

Another significant concern for the accounting industry is attacks. These attacks involve encrypting data and demanding extortion payments (Kafi & Adnan, 2022; Bodepudi et al., 2019; Mandapuram, 2017; Gutlapalli, 2016). The "Data Breach Investigations Report" by Verizon provides insights into the prevalence and impact of ransomware attacks. It emphasizes how such attacks disrupt accounting operations, including transactions and service delivery (Jartelius, 2020). Understanding these attacks' nature is crucial for developing strategies to prevent and respond to them.

When it comes to cybersecurity, the focus is often on threats. However, it's essential not to overlook the risks insiders pose regarding accounting data security. The "Insider Threat Report" from the CERT Division of the Software Engineering Institute sheds light on the motivations and behaviors of insiders. Offers recommendations for preventing and detecting such threats (Noever, 2019). This research highlights the significance of promoting a security culture within accounting organizations through employee awareness and training programs.

Studies and industry guidelines are available that provide recommendations for safeguarding financial information in the digital realm (Mandapuram & Hosen, 2018; Mandapuram, 2016; Gutlapalli et al., 2019). For instance, the American Institute of Certified Public Accountants (AICPA) has published the "Cybersecurity Risk Management Framework," which presents an approach for identifying, protecting against, detecting, responding to, and recovering from cybersecurity incidents (Hyde, 2016). This framework encompasses best practices specifically tailored to the accounting profession. Academic research has extensively examined aspects of cybersecurity in accounting, including access controls, encryption techniques, network monitoring systems, and incident response strategies (Chang et al., 2018; Simkins et al., 2020). These studies contribute to our understanding of cybersecurity practices and how they can be applied in accounting.

By synthesizing information from these literature sources, this article aims to provide an overview of cybersecurity challenges, risks, and best practices for protecting accounting data. The knowledge obtained from these research contributions will provide information for the case studies and recommendations. This will help accounting professionals and organizations improve cybersecurity and safeguard sensitive financial information effectively.

Types of Cyber Incidents

Cyber incidents can indeed occur due to both artificial causes and natural disasters. However, this article focuses explicitly on manufactured attacks or incidents resulting

from human error. The intention is to highlight the cybersecurity risks human actions pose and provide insights into mitigating such risks. According to a report by IBM Security, human error remains a significant contributor to data breaches, accounting for a substantial percentage of incidents (IBM Security, 2022). This highlights the importance of addressing human-related factors in cybersecurity strategies. The Verizon Data Breach Investigations Report reveals that most data breaches involve human error, such as misconfiguration, phishing, or inadvertent data exposure (Pritam, 2020). The report emphasizes the need for organizations to educate employees, implement robust security practices, and proactively manage human-related risks. Phishing Attacks: Phishing involves fraudulent attempts to obtain sensitive information, such as usernames, passwords, or financial details, by masquerading as a trustworthy entity in emails, messages, or websites. The typical cyber-attacks are:

Phishing Attacks: Phishing attacks involve deceptive emails, messages, or websites that trick individuals into providing sensitive information. Attackers often masquerade as trustworthy entities to obtain usernames, passwords, and financial details. Phishing attacks can lead to unauthorized access to accounting data, potentially compromising security (APWG, 2022).

Advanced Persistent Threats (APTs): APTs are sophisticated, long-term cyber-attacks targeting organizations or individuals. These attacks involve a stealthy infiltration into the target's network, persistent monitoring of activities, and the exfiltration of sensitive data over an extended period. APTs are characterized by their advanced techniques, customized strategies, and ability to evade traditional security measures (RED-GOAT, 2019).

Broken Access Control: Broken access control attackers can exploit vulnerabilities to gain unauthorized access to sensitive data. These vulnerabilities can lead to unauthorized disclosure, modification, or destruction of critical information, posing significant risks to accounting data and compromising its integrity and confidentiality (OWASP, 2021).

Broken Authentication: Exploiting broken authentication vulnerabilities allows attackers to gain control over user accounts, potentially compromising accounting data. Such exposures can result from weak passwords, session management flaws, or insecure authentication mechanisms, providing unauthorized access to sensitive information (OWASP, 2021).

Cross-Site Scripting: Cross-site scripting (XSS) attacks occur when malicious scripts are injected into web applications, which are then executed by users' browsers. Threat actors can exploit XSS vulnerabilities to access user accounts, collect browser histories, and distribute malware, putting accounting information at risk (OWASP, 2021).

Data Breaches: Data breaches involve unauthorized access or disclosure of sensitive information, including personal or financial data. For accounting information, data breaches can result in financial fraud, identity theft, reputational damage, and regulatory compliance issues, posing significant risks to individuals and organizations (Pritam, 2020).

Insider Threats: Insider threats refer to individuals within an organization misusing their access privileges to compromise data or systems. This can include intentional actions, such as data theft or unauthorized access, and unintentional actions due to negligence or human error. Insider threats pose a significant risk to accounting information, as insiders often have access to critical financial data and systems (Noever, 2019).

Malware Attacks: Malware attacks involve deploying malicious software, such as ransomware, viruses, or spyware, to infiltrate systems, steal sensitive data, or disrupt operations. For accounting information, malware attacks can result in financial losses, data compromise, and operational disruptions that impact financial processes (Pritam, 2020).

Security Misconfiguration: Security misconfiguration occurs when systems, frameworks, or applications are improperly configured, leaving them vulnerable to attacks. Misconfigurations can expose accounting data to unauthorized access, enabling attackers to compromise sensitive information and exploit system weaknesses (OWASP, 2021).

Sensitive Data Exposure: Sensitive data exposure can occur when insecure transmission methods are used for transmitting data, such as usernames and passwords, through certain APIs. Attackers can intercept and exploit this exposed data, potentially compromising the security of accounting information (OWASP, 2021).

SQL Injection: SQL injection attacks exploit vulnerabilities in web applications that allow malicious SQL statements to be injected. Successful attacks can grant unauthorized access to databases and critical data, enabling attackers to manipulate or steal accounting information (OWASP, 2021).

XML External Entities: XML external entity attacks occur when attackers upload or include malicious XML content in insecure code or dependencies. By leveraging these vulnerabilities, attackers can gain unauthorized access to sensitive information, potentially compromising accounting data (OWASP, 2021).

Organizations must comprehend the threats associated with these attacks and implement appropriate security measures and best practices to protect accounting information from potential threats.

How do those Attacks Pose Threats to Accounting Information?

Cyber-attacks pose significant threats to the security and integrity of accounting information (Reddy et al., 2020). These malicious activities exploit vulnerabilities in digital systems, compromising sensitive financial data and potentially disrupting financial operations. Understanding the specific ways these attacks target accounting information is crucial for developing effective cybersecurity measures and safeguarding the integrity and confidentiality of financial data. The categorical impact of cyber-attack are:

Malware Attacks: Malware attacks, such as ransomware, viruses, or spyware, can severely impact accounting information. Malicious software can infiltrate accounting systems, steal financial data, disrupt operations, or encrypt critical financial records. These attacks can lead to financial losses, operational disruptions, or the compromise of economic data, posing significant risks to accounting information's accuracy, availability, and integrity.

Phishing Attacks: Phishing attacks targeting accounting professionals can have dire consequences for accounting information security. By tricking users into revealing their login credentials or financial details, attackers can gain unauthorized access to economic systems, manipulate financial data, or carry out fraudulent transactions. Phishing attacks can lead to unauthorized access, financial fraud, or the compromise of sensitive financial information.

Advanced Persistent Threats (APTs): APTs are highly sophisticated and targeted attacks that aim to infiltrate specific organizations or individuals over an extended period. APTs pose a grave danger to accounting information as they involve stealthy infiltration, persistent monitoring, and data exfiltration. By compromising accounting systems or networks, attackers can access sensitive financial data, potentially leading to financial fraud, intellectual property theft, and compromise of financial transactions.

Broken Access Control: Attacks exploiting broken access control vulnerabilities can have severe consequences for accounting information. Unauthorized access to critical financial data or systems can lead to the unauthorized disclosure, modification, or destruction of sensitive accounting information. This can result in financial inaccuracies, fraudulent activities, or unauthorized transactions, jeopardizing the integrity and accuracy of financial records.

Broken Authentication: Exploiting broken authentication vulnerabilities can enable attackers to gain control over user accounts, potentially compromising accounting data. With unauthorized access to authenticated accounts, attackers can manipulate financial data, falsify transactions, or impersonate authorized users, leading to financial losses, data corruption, or regulatory non-compliance.

Cross-Site Scripting: Cross-site scripting attacks can have detrimental effects on accounting information. By injecting malicious scripts into vulnerable web applications, intruders can take control of user accounts and collect sensitive financial data, including usernames, passwords, and financial transactions. This can result in unauthorized access to economic systems, fraudulent activities, or the manipulation of accounting data, putting the accuracy and security of financial information at risk.

Data Breaches: Data breaches involving unauthorized access or disclosure of sensitive accounting information can have far-reaching consequences. Breached accounting data, such as financial records, payroll information, or client details, can be exploited for financial fraud, identity theft, or corporate espionage. The exposure of such information can lead to reputational damage, financial losses, regulatory penalties, and compromised business relationships.

Insider Threats: Insider threats pose significant dangers to accounting information, involving individuals within an organization misusing their access privileges. Insiders, including employees, contractors, or partners, may intentionally or unintentionally compromise accounting data. Unauthorized access, data theft, or the manipulation of financial records by insiders can result in financial inaccuracies, fraudulent activities, or the compromise of financial controls and compliance measures.

Cases of Cyber Attacks, Understanding Threats

Cyber-attacks have become increasingly prevalent in today's digital landscape, posing significant risks to organizations across various sectors, including finance, healthcare, government, and more. These attacks, orchestrated by threat actors with diverse motivations, target critical systems, sensitive data, and financial information, leading to financial losses, reputational damage, and disruptions to operations. Understanding the nature and impact of these cyber-attacks is crucial for organizations to develop effective cybersecurity strategies and safeguards. This article explores notable cyber-attack cases, highlighting their consequences and providing insights into the evolving threat landscape. By examining these cases, organizations can gain valuable knowledge to enhance their defenses and protect against emerging cyber threats. Some cyber incidents in recent years are:

Equifax Data Breach (2017): In 2017, Equifax, one of the largest credit reporting agencies, experienced a significant data breach that exposed the sensitive personal information of approximately 147 million individuals. The breach included names, Social

Security numbers, birth dates, and in some cases, credit card information. This breach underscored the risks to accounting information and highlighted the importance of data protection in the financial sector.

NotPetya Ransomware Attack (2017): The NotPetya ransomware attack 2017 affected numerous organizations globally, including financial institutions. The attack initially targeted businesses in Ukraine but quickly spread worldwide. It caused widespread disruption, including temporary shutdowns of critical economic systems and significant financial losses. This incident highlighted the interconnectedness of financial networks and the potential consequences for accounting data in the event of a large-scale attack (CNN, 2017).

Capital One Data Breach (2019): In 2019, Capital One, a significant financial institution, experienced a data breach that exposed the personal information of approximately 106 million customers. The breach included names, addresses, credit scores, and other financial data. The incident highlighted the importance of robust cybersecurity measures to safeguard accounting information and the potential risks posed by insider threats.

JPMorgan Chase Cyber Attack (2014): In 2014, JPMorgan Chase Bank, one of the prominent financial institutions in the United States, experienced a significant cyber-attack. The attack compromised the personal information of around 76 million individuals or households and 7 million small businesses. While the motive behind the attack was unclear, it highlighted the vulnerability of financial institutions to cyber threats.

Bangladesh Bank Heist (2016): In 2016, cybercriminals successfully targeted the Bangladesh Bank, the central bank of Bangladesh, in what is considered one of the largest bank heists in history. The attackers used malware to access the bank's systems and attempted to transfer nearly $1 billion from its account held at the Federal Reserve Bank of New York. Although most transactions were blocked, approximately $81 million was transferred to fraudulent accounts (BBC News, 2016).

WannaCry Ransomware Attack (2017): The WannaCry ransomware attack 2017 affected numerous organizations worldwide, including financial institutions. The attack exploited a vulnerability in Windows operating systems and encrypted files on infected computers, demanding ransom payments in Bitcoin. While the economic impact varied across institutions, the attack caused significant disruptions and highlighted the need for robust cybersecurity measures in the financial sector (BBC News, 2016).

How were the Attacks done? The Intruders' Way

Understanding how cybercriminals operate is essential for organizations and individuals to defend against their malicious activities. Cybercriminals employ various techniques, tools, and strategies to exploit vulnerabilities and gain unauthorized access to systems, steal sensitive data, or disrupt operations. This article delves into the world of cybercriminals, shedding light on their methods, motivations, and tactics to carry out cyber-attacks. Following is the preamble about how cyber-attacks took place in the cases mentioned in this article.

Equifax Data Breach (2017): The Equifax data breach involved attackers exploiting a vulnerability in the company's website application. By gaining unauthorized access, they could extract millions of individuals' sensitive personal information.

NotPetya Ransomware Attack (2017): The NotPetya ransomware attack spread through a malicious software update of a famous Ukrainian tax accounting software. It quickly infected systems globally, encrypting files and demanding ransom payments in Bitcoin. However, it is essential to note that NotPetya was more destructive than profit-oriented, causing significant disruption rather than focusing solely on financial gain (Wired, 2017).

Capital One Data Breach (2019): In the Capital One data breach, a former Amazon Web Services (AWS) contractor employee exploited a misconfiguration in a web application firewall, gaining unauthorized access to customer data. The attacker exhilarated the personal information of millions of Capital One customers.

JPMorgan Chase Cyber Attack (2014): The JPMorgan Chase cyber-attack was attributed to a group of hackers believed to be based in Russia. The attackers gained unauthorized access to the bank's network by exploiting vulnerabilities in the bank's website and bypassing security measures. They managed to infiltrate the bank's systems and access sensitive data, including customer information.

Bangladesh Bank Heist (2016): In the Bangladesh Bank heist, cybercriminals used sophisticated techniques to compromise the bank's security systems. They sent fraudulent payment instructions through the SWIFT network, an interbank messaging system, to transfer funds from the bank's account held at the Federal Reserve Bank of New York. The attackers used malware to manipulate the bank's records and cover their tracks (BBC News, 2016).

WannaCry Ransomware Attack (2017): The WannaCry ransomware attack spread globally by exploiting a vulnerability in Microsoft Windows operating systems. The attack used a worm-like propagation method to infect vulnerable computers connected to the internet.

Once infected, the ransomware encrypted files and demanded ransom payments in Bitcoin. The attack affected numerous organizations, including healthcare institutions and financial entities (BBC News, 2016).

How were They Vulnerable to Attacks? The Attack Vectors

This paper examines the cases of Equifax, Marriott, NotPetya, Capital One, JPMorgan Chase, Bangladesh Bank, and WannaCry to provide guidelines for securing accounting information. Comprehensive analysis reveals various technical and non-technical weaknesses that contributed to these attacks. To ensure easy comprehension across disciplines, this research utilizes accessible terminology:

The Equifax data breach exposed the personal and financial information of approximately 147 million individuals. One of the weaknesses exploited by the attackers was a vulnerability in the Apache Struts web application framework (US Government Accountability Office, 2019). The attackers gained unauthorized access to Equifax's system by exploiting this vulnerability and exfiltrated sensitive data over an extended period.

The NotPetya ransomware attack caused significant disruption to various organizations worldwide. It spread rapidly by exploiting the EternalBlue vulnerability, initially developed by the National Security Agency (NSA) and leaked by a hacking group called Shadow Brokers (US-CERT, 2018). NotPetya encrypted the targeted systems, rendering them inoperable, and demanded ransom payments for data recovery. The attack highlighted the importance of promptly applying security patches and updates to address known vulnerabilities.

The Capital One data breach affected over 100 million customers and involved unauthorized credit card application data access. The attacker exploited a server-side request forgery (SSRF) vulnerability, which allowed them to access a misconfigured web application firewall (WAF) to extract sensitive information (Capital One, 2019). The WAF configuration's weakness and the web application's vulnerability exposed customer data to the attacker.

The cyber-attack on JPMorgan Chase targeted the bank's internal network and compromised the personal information of 76 million households and 7 million small businesses. The attackers gained initial access through a spear-phishing campaign directed at bank employees (United States Department of Justice, 2015). The attack's success was attributed to weaknesses in the bank's email security and employee awareness, allowing the attackers to infiltrate the network.

The Bangladesh Bank heist involved the attempted theft of $951 million from the bank's account at the Federal Reserve Bank of New York. The attackers exploited the bank's security infrastructure vulnerabilities, including weak network controls and a lack of two-factor authentication (Bukth & Huda, 2017). This allowed them to initiate fraudulent transactions and transfer funds to accounts in other countries.

The WannaCry ransomware attack affected hundreds of thousands of computers globally, including those in critical sectors such as healthcare and finance. It exploited a vulnerability in the Windows operating system called EternalBlue, which was also leaked by the Shadow Brokers (US-CERT, 2018). WannaCry spreads rapidly across networks, encrypting files and demanding ransom payments. The attack highlighted the significance of promptly applying security patches and updates to protect systems from known vulnerabilities.

Securing Accounting Information

Securing accounting information from cyber-attacks is crucial to protect sensitive financial data's confidentiality, integrity, and availability. In today's digital landscape, where cyber threats continue to evolve, organizations must adopt proactive measures and best practices to safeguard their accounting systems and data (Bodepudi et al., 2021). Here are some critical steps that can be implemented:

Strong Access Controls: Implement robust access controls to limit access to accounting systems and sensitive financial data. This includes enforcing strong passwords, multi-factor authentication, role-based access controls, and regular review and revocation of user access rights (National Institute of Standards and Technology, 2018).

Regular Software Patching and Updates: Keep accounting software and systems updated with the latest patches and security updates. Promptly applying patches helps address known vulnerabilities and protect against exploitation by cyber criminals (United States Computer Emergency Readiness Team, 2018).

Data Encryption: Employ encryption techniques to protect sensitive accounting data during storage and transmission. Encryption safeguards data from unauthorized access and ensures that even if data is intercepted, it remains unintelligible to unauthorized individuals (National Institute of Standards and Technology, 2018).

Employee Awareness and Training: Provide employees with comprehensive cybersecurity awareness and training programs. This should cover topics such as recognizing phishing emails, secure password practices, social engineering awareness, and the importance of data protection in the accounting environment (SANS Institute, n.d.).

Regular Data Backups: Maintain regular backups of accounting data and store them securely offline or in a separate location. Regular backups ensure data availability in case of a cyber-attack, system failure, or data loss event (United States Computer Emergency Readiness Team, 2018).

Network Segmentation: Implement network segmentation to separate critical accounting systems from the rest of the network infrastructure. This helps contain potential breaches and limits the lateral movement of attackers within the network (National Institute of Standards and Technology, 2018).

Intrusion Detection and Prevention Systems (IDPS): Deploy IDPS solutions to monitor network traffic, detect suspicious activities, and block or mitigate potential cyber threats. IDPS can help identify and respond to attacks in real time, minimizing the impact on accounting systems (SANS Institute, n.d.).

It is important to note that these measures should be implemented as part of a comprehensive cybersecurity strategy tailored to the specific needs and risks of the organization. The NIST Cybersecurity Framework can be instrumental in securing accounting information by offering a structured approach to identify, protect, detect, respond to, and recover from cybersecurity incidents (NIST, 2018). Here's how it can help:

Risk Assessment: The framework assists organizations in conducting risk assessments specific to their accounting systems and data. This involves identifying and prioritizing cybersecurity risks, assessing potential vulnerabilities, and understanding the impact of a breach on accounting information (NIST, 2018).

Controls and Safeguards: The framework provides a set of commands and safeguards that organizations can implement to protect accounting information. This includes access controls, encryption techniques, secure configurations, and network segmentation to safeguard sensitive financial data (NIST, 2018).

Incident Detection and Response: The framework emphasizes the importance of implementing robust detection mechanisms to identify cybersecurity incidents promptly. This involves deploying security monitoring systems and intrusion detection systems and establishing incident response procedures to minimize the impact of a breach on accounting information (NIST, 2018).

Continuous Monitoring: The NIST framework promotes constant monitoring of cybersecurity controls to ensure their effectiveness over time. This includes regularly assessing and reviewing the security posture of accounting systems, monitoring for vulnerabilities, and addressing emerging threats promptly (NIST, 2018).

Cybersecurity Training and Awareness: The framework recognizes the critical role of employees in maintaining cybersecurity. It encourages organizations to provide staff cybersecurity training and awareness programs, ensuring they understand their responsibilities in protecting accounting information and can identify and report potential threats (NIST, 2018).

Implementing the NIST Cybersecurity Framework can help secure accounting information by providing a systematic and comprehensive approach to managing cybersecurity risks. It enables organizations to establish a strong cybersecurity posture, align their practices with industry standards, and enhance their ability to prevent, detect, and respond to cyber threats. Besides, the SANS Institute, a trusted authority in cybersecurity education and research, provides comprehensive guidance on various aspects of information security. Their recommended policies cover access controls, incident response planning, security awareness training, and secure configuration management (SANS Institute, n.d.). These policies align with industry best practices and can help organizations bolster the security of their accounting information.

The International Federation of Accountants, a global accounting organization, emphasizes the need for robust cybersecurity practices in protecting financial information. They have developed frameworks and guidelines, such as the IFAC Cybersecurity Framework and the International Good Practice Guide on Cybersecurity, which provide actionable recommendations and strategies to safeguard accounting data (IFAC, 2019). These resources offer a structured approach to assessing cybersecurity risks, implementing appropriate controls, and ensuring the resilience of accounting information systems.

Adhering to the policies prescribed by the SANS Institute and the International Federation of Accountants, organizations can enhance the security of their accounting information. These policies provide a framework for implementing essential security controls, establishing incident response capabilities, promoting employee awareness, and adopting industry-recognized best practices. Implementing these policies can significantly mitigate the risk of cyber threats and help safeguard accounting information's confidentiality, integrity, and availability. Through implementing these measures and best practices, organizations can establish a robust cybersecurity posture to safeguard their accounting information from cyber-attacks and maintain the trust of stakeholders.

Technical Tools for Securing Accounting Information

There are specialized security tools that play a vital role in safeguarding information and keeping accounting data secure from cyber-attacks. Let's take a look at some of these tools and their specific functions:

Antivirus Software: Antivirus software plays a role in detecting, preventing, and removing software like viruses, worms, and Trojans. Its primary function is to identify and eliminate known malware threats to files, programs, and systems. By updating virus definitions, antivirus software provides a defense against common cyber threats (Symantec, n.d.).

Web Application Firewall (WAF): A web application firewall is a security tool that filters and monitors HTTP traffic between a web application and the internet. Its purpose is to safeguard web applications from exploited attack vectors such as SQL injections, cross-site scripting (XSS), and cross-site request forgery (CSRF). WAFs utilize traffic filtering, application layer security policies, and anomaly detection to protect web applications (Cloudflare, n.d.).

Wireless Network Security: Wireless network security includes the measures taken to safeguard networks from access. To enhance the security of Wi-Fi networks, it is essential to use encryption protocols, like WPA2 or WPA3, create passwords, and turn off any unnecessary services or features that may introduce vulnerabilities. When it comes to network switches, they play a role in managing and controlling network traffic. They enable the creation of LANs (VLANs). Enforce access control policies to prevent unauthorized access to sensitive resources. By handling network traffic, switches help safeguard accounting information from threats (Cisco, n.d.).

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS): IDS and IPS are security tools designed to detect and prevent access or malicious activities within a network. The IDS continuously monitors network traffic alerting administrators of any behavior. The IPS goes further by blocking or mitigating identified threats to enhance network security (Cisco, n.d.).

Security Information and Event Management (SIEM) System: SIEM systems collect and analyze security event logs from sources within an organization's network infrastructure. These systems provide real-time monitoring, threat detection, and incident response capabilities by correlating and analyzing security events. This empowers security teams to effectively identify and respond to threats promptly (Gartner, n.d.).

Data Loss Prevention (DLP) System: DLP systems assist organizations in safeguarding data from unauthorized disclosure or loss. These systems regulate data flow within the network enforcing policies to prevent data leakage. Additionally, they can. Prevent data transmission outside the organization's boundaries (Symantec, n.d.).

Two-Factor Authentication (2FA): Two-factor authentication enhances security measures by requiring users to provide two forms of identification before accessing a system or application. This additional layer of authentication helps ensure that authorized individuals gain access, adding an extra level of protection against unauthorized access attempts. In situations where users need to provide both something they're aware of, such as a password, and something they possess, like a code sent to their mobile device (NIST, 2020), it becomes crucial to effectively deal with known weaknesses and reduce the likelihood of being exploited. A fundamental approach to achieve this is by updating and patching software and systems. By establishing a process for managing patches, security updates can be applied promptly, thus minimizing the risk of cyber threats (US-CERT, 2018).

Network Firewalls: Firewalls are a barrier between an internal network and external networks or the internet. They monitor and control incoming and outgoing network traffic based on predefined security rules, helping to prevent unauthorized access and protect against malicious activities (Microsoft, n.d.).

These technical tools, endpoint protection solutions, network segmentation, and secure coding practices contribute to a comprehensive cybersecurity posture, helping protect against cyber threats and safeguard sensitive information.

Endpoint Protection Solutions: The primary purpose of endpoint protection solutions is to safeguard endpoints like computers, laptops, servers, and mobile devices from various cyber threats. These solutions typically include antivirus software, anti-malware tools, and firewalls that detect and block programs. They also come with real-time threat monitoring, behavior-based detection, and vulnerability management to identify and prevent endpoint attacks. By ensuring endpoints' security, these solutions help reduce the risk of malware infections, unauthorized access, and data breaches.

Network Segmentation: Network segmentation involves dividing a network into isolated segments or subnetworks. Each piece is then logical. Restricted from accessing other components creates barriers that limit the spread of cyber threats within the network. When organizations implement network segmentation, they can contain breaches, reduce the movement of attackers within the web, and minimize the impact of a successful attack by confining it to a specific segment. Overall this approach enhances network security. Protects critical assets, such as accounting information, from unauthorized access (Cisco, n.d.).

Secure Coding Practices: Secure coding practices encompass a set of guidelines, principles, and techniques used throughout the software development process to mitigate vulnerabilities and weaknesses that cyber threats can exploit. These best practices involve ensuring that the input is validated, adequately handled sensitive data, secure authentication, access controls are in place, errors are handled appropriately, and regular security testing is conducted. By following coding practices, software developers can minimize the chances of introducing vulnerabilities into applications and systems, thus reducing the potential for attackers to exploit them (OWASP, 2021).

These technical security tools play a role in safeguarding information by utilizing various mechanisms and protocols to detect and prevent cyber threats. They aid in minimizing risks to accounting information by detecting malware, filtering traffic, encrypting data managing access control, and addressing vulnerabilities.

Virtual Private Network (VPN) A VPN can significantly enhance cybersecurity by providing an encrypted connection for internet communications. Here's how a VPN contributes to cybersecurity:

Data Encryption: With a VPN, a secure tunnel is established between the user's device and the VPN server. This tunnel ensures that all transmitted data is encrypted, making it impossible for unauthorized individuals to intercept or access it. Encrypting information like accounting data prevents any compromises during transmission (Cisco, n.d.).

Privacy and Anonymity: VPNs also play a role in safeguarding user privacy and anonymity by concealing their IP address and location. When connected to a VPN, your internet activity appears to originate from the VPN server's location, making it challenging for cyber attackers to track or trace your activities.

Protection on Public Wi-Fi: VPNs are beneficial when connecting to the internet on Wi-Fi networks in cafes or airports. These networks are often insecure and susceptible to eavesdropping or data interception. By encrypting your data traffic, a VPN provides a layer of security protecting your accounting information from potential threats on public Wi-Fi networks.

Bypassing Geographical Restrictions: Apart from the security benefits, VPNs can also assist in bypassing restrictions or censorship. VPNs are a resource for accessing accounting data and conducting business activities in regions where specific websites or services are restricted or limited.

By employing encryption techniques, ensuring privacy and anonymity, and safeguarding internet connections, VPNs play a role in bolstering cybersecurity measures and protecting accounting information against potential threats.

Securing Accounting Information: Cases and Process

Here are some known organizations that have implemented effective cybersecurity measures to ensure the security of their accounting information:

JPMorgan Chase: JPMorgan Chase has gained recognition for its strong focus on cybersecurity, aiming to safeguard financial and customer data. The company invests in cutting-edge cybersecurity technologies, including advanced threat detection systems, network monitoring tools, and encryption mechanisms. Moreover, JPMorgan Chase consistently conducts cybersecurity training programs. Promotes a culture of security awareness among its employees (Glazer, 2015).

Deloitte: Deloitte, one of the leading professional services firms, places importance on cybersecurity to protect sensitive financial information. The firm employs various security measures, such as implementing multi-factor authentication, encryption techniques, and intrusion detection systems to safeguard client data. Deloitte has also established a team dedicated to cybersecurity, continuously monitoring and responding to emerging threats (Deloitte, n.d.).

Citigroup: Citigroup has implemented cybersecurity processes and cutting-edge technologies to ensure the security of its accounting information. The organization utilizes security controls such as real-time monitoring, access controls, and data encryption. Citigroup also leverages threat intelligence. Maintains a team of cybersecurity experts who proactively identify and mitigate potential risks (Citigroup, 2019).

Microsoft: As a technology giant, Microsoft prioritizes cybersecurity throughout its operations. The company adopts measures to protect its systems and sensitive data from cyber threats. The company has put in place security measures to safeguard its financial data. This includes software updates, patches, advanced authentication methods, and encryption technologies. Microsoft also shares threat intelligence and collaborates with industry partners to stay ahead of evolving cyber threats (Microsoft, n.d.).

Ernst & Young (EY): EY focuses on maintaining a cybersecurity stance to protect the financial information of its clients. The firm uses security controls like intrusion detection systems, network segmentation, and employee training programs. EY also conducts risk assessments and security audits to identify vulnerabilities while ensuring compliance with industry regulations (EY, n.d.).

These organizations emphasize cybersecurity by employing technical measures, employee training, and proactive monitoring to safeguard their accounting information from cyber threats.

What did They Do? Cases of Notable Cyber-attacks

Several prominent organizations, including Equifax, NotPetya, Capital One, JPMorgan Chase, Bangladesh Bank, and WannaCry, have taken cybersecurity measures to safeguard their systems and sensitive information after successful cyber-attacks. These organizations employ a combination of strategies and best practices to strengthen their cybersecurity defenses and mitigate risks.

Equifax, a consumer credit reporting agency, has prioritized fortifying its cybersecurity measures after experiencing a data breach in 2017. The company has implemented security protocols such as network segmentation, encryption, and multi-factor authentication to safeguard customer data (Equifax, 2021).

NotPetya was a destructive ransomware attack that targeted numerous organizations worldwide. It exploited vulnerabilities in systems and deployed malicious software to encrypt data. This incident underscored the

criticality of patching and vulnerability management in protecting against such threats (FORTRA, 2017).

Capital One, a financial institution, adopts a multi-layered cybersecurity strategy to safeguard customer and financial data. JP Morgan Chase, one of the banks in the United States, places great importance on ensuring the security of its systems and networks. The company invests in security measures, enforces strong access controls, and maintains a dedicated team of cybersecurity experts to safeguard its systems and protect customer data (JPMorgan Chase).

In 2016 ***Bangladesh Bank*** experienced a publicized cyber heist in which hackers exploited weaknesses in the bank's systems to steal millions of dollars. This incident highlighted the need for robust security controls, continuous monitoring, and swift incident response to prevent and detect such attacks (BBC News, 2016).

WannaCry, a spread ransomware attack, specifically targeted vulnerable systems using a mechanism that resembled a worm. The attack took advantage of a vulnerability in Windows, underscoring the importance of software updates and the application of security patches (US-CERT, 2020).

These organizations prioritize cybersecurity and deploy various technical strategies to safeguard their systems and data from cyber threats. They implement network segmentation, encryption techniques, real-time monitoring, and vulnerability management as part of their security strategies.

RECOMMENDATIONS

Securing accounting information against evolving cyber threats requires an effort, and it's crucial to have a layered defense strategy in place. While the following recommendations offer guidance, it's essential to consider organizations' specific needs and requirements when implementing cybersecurity measures.

Strong Access Controls: It is crucial to implement strong access controls to enhance the security of accounting systems and protect financial data. This entails enforcing password policies utilizing multi-factor authentication assigning access based on roles and regularly reviewing and revoking user access rights.

Regular Software Patching and Updates: Keeping accounting software and systems up to date with the patches and security updates is paramount. This practice helps to address known vulnerabilities and safeguards against exploitation by cybercriminals.

Data Encryption: To protect accounting data, encryption techniques are recommended throughout its storage and transmission. Encryption protects against access, ensuring that intercepted data remains incomprehensible to unauthorized individuals.

Employee Awareness and Training: To foster a culture of cybersecurity within the accounting environment, it is essential to provide employee awareness and training programs. These programs should cover topics like identifying phishing emails, practicing password management, recognizing social engineering tactics, and understanding the significance of data protection.

Regular Data Backups: Maintain regular backups of accounting data and store them securely offline or in a separate location. Regular backups ensure data availability in case of a cyber-attack, system failure, or data loss event.

Network Segmentation: To enhance security measures, it is recommended to implement network segmentation. This involves separating accounting systems from the rest of the network infrastructure. This strategy helps contain breaches and restricts attackers' ability to move laterally within the network.

Intrusion Detection and Prevention Systems (IDPS): Deploying Intrusion Detection and Prevention Systems (IDPS) can significantly contribute to network security. These systems monitor network traffic, detect any activities and take necessary actions to block or mitigate potential cyber threats. By utilizing IDPS, accounting systems can be safeguarded in time, minimizing the impact of attacks.

Regular Risk Assessments: Regularly assess and evaluate the organization's risk landscape to identify vulnerabilities and potential threats to accounting information. By conducting thorough risk assessments, organizations can understand their unique risks and prioritize security efforts accordingly. This helps identify improvement areas and implement targeted security controls.

Foster a Culture of Security: Humanize the cybersecurity approach by fostering a security culture. This involves creating awareness among employees about the importance of protecting accounting information and their role in maintaining security. Encourage a proactive mindset towards cybersecurity, where employees feel comfortable reporting potential risks or incidents.

Secure Configuration Management: Implement certain configuration management practices for accounting systems and software. Ensure systems are correctly configured, unnecessary services are disabled, and only essential software and functionalities are enabled. Regularly update and patch software to address known vulnerabilities and keep systems secure.

Incident Response Plan: Develop a well-defined incident response plan specific to cyber-attacks on accounting information. This plan should outline the steps to be taken during a security incident, including the roles and responsibilities of key personnel, communication protocols, and recovery procedures. Regularly check and update the plan to ensure its effectiveness.

Continuous Monitoring: Implement continuous monitoring practices to identify and respond to possible threats in real time. Deploy security monitoring tools, such as intrusion detection systems and security information and event management (SIEM) solutions, to monitor the network for suspicious activities and indicators of compromise. This allows for early detection and swift response to potential security incidents.

Vendor Risk Management: Pay close attention to the security practices of third-party vendors and service providers with access to accounting information. Establish a robust vendor risk management program, which includes conducting due diligence assessments, incorporating security requirements in contracts, and regularly monitoring vendor compliance. This helps ensure that shared data remains secure throughout the supply chain.

Employee Cybersecurity Training: Provide regular and comprehensive cybersecurity training for all employees. Human error remains a significant factor in cyber incidents, so educating staff about emerging threats, phishing awareness, secure computing practices, and incident reporting is crucial. Organizations can create a robust human firewall against cyber threats *by enhancing employees' cybersecurity knowledge and skills.*

Compliance with Regulations and Standards: Stay current with relevant regulations and industry standards governing the protection of accounting information. Compliance with frameworks such as GDPR or PCI DSS may be necessary depending on the organization's industry and geographical location. Ensure that appropriate security controls and practices are in place to meet regulatory requirements.

REFERENCES

APWG. (2022). *Phishing Activity Trends Report*. https://apwg.org/trendsreports/

BBC News. (2016). *Bangladesh bank hackers fail in bid to net $1bn*. https://www.bbc.co.uk/news/technology-35773061

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2019). Voice Recognition Systems in the Cloud Networks: Has It Reached Its Full Potential?. *Asian Journal of Applied Science and Engineering*, *8*(1), 51–60. https://doi.org/10.18034/ajase.v8i1.12

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2021). Algorithm Policy for the Authentication of Indirect Fingerprints Used in Cloud Computing. *American Journal of Trade and Policy*, *8*(3), 231–238. https://doi.org/10.18034/ajtp.v8i3.651

Bukth, T., & Huda, S. S. (2017). *The soft threat: The story of the Bangladesh bank reserve heist*. SAGE Publications. https://doi.org/10.4135/9781526411228

Capital One. (2019). *Capital One Announces Data Security Incident.* https://www.prnewswire.com/news-releases/capital-one-announces-data-security-incident-300892738.html

Chang, V., Walters, R. J., & Wills, G. (2018). Cybercrime and accounting information systems: A novel research direction. *Journal of Computer Information Systems*, 58(4), 334–343.

CISCO. (n.d.). *What Is a Network Switch?* https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html

Citigroup. (2019.). *Cybersecurity: protective measures treasuries should be taking.* https://www.citibank.com/tts/solutions/cybersecurity/

Cloudflare. (n.d.). *What Is a Web Application Firewall (WAF)?* https://developers.cloudflare.com/waf/about/

Deloitte. (n.d.). *Cybersecurity and Privacy Awareness.* https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose/cybersecurity-an-privacy-awareness.html

Equifax. (2021). *Support Regulatory & Security Compliance*. https://www.equifax.com/business/identity-fraud/support-regulatory-security-compliance/

Ernst & Young (EY). (n.d.). *Cybersecurity.* https://www.ey.com/en_uk/cybersecurity

FORTRA. (2017). *NotPetya: Timeline of a Ransomworm.* https://www.tripwire.com/state-of-security/notpetya-timeline-of-a-ransomworm

Glazer, E. (2015). J.P. Morgan to Accelerate Timeline for Cybersecurity Spending Boost. *The Wall Street Journal*. https://www.wsj.com/articles/j-p-morgan-to-accelerate-timeline-for-cybersecurity-spending-boost-1438641746

Gutlapalli, S. S. (2016). Commercial Applications of Blockchain and Distributed Ledger Technology. *Engineering International*, *4*(2), 89–94. https://doi.org/10.18034/ei.v4i2.653

Gutlapalli, S. S. (2017). Analysis of Multimodal Data Using Deep Learning and Machine Learning. *Asian Journal of Humanity, Art and Literature*, *4*(2), 171–176. https://doi.org/10.18034/ajhal.v4i2.658

Gutlapalli, S. S., Mandapuram, M., Reddy, M., & Bodepudi, A. (2019). Evaluation of Hospital Information Systems (HIS) in terms of their Suitability for Tasks. *Malaysian Journal of Medical and Biological Research*, *6*(2), 143–150. https://doi.org/10.18034/mjmbr.v6i2.661

Hyde, J. (2016). AICPA Unveils Cybersecurity Risk Management Reporting Framework. *AICPA & CIMA*.

https://www.aicpa-cima.com/news/article/aicpa-unveils-cybersecurity-risk-management-reporting-framework

IBM Security. (2022). *Cost of a Data Breach Report.* https://www.ibm.com/downloads/cas/3R8N1DZJ

Jartelius, M. (2020). The 2020 Data Breach Investigations Report–a CSO's perspective. *Network Security*, *2020*(7), 9-12.

JPMorgan Chase. *Protecting Our Systems and Customer Information.* https://www.jpmorgan.com/insights/fraud/fraud-protection/how-to-protect-and-secure-customer-data

Kafi, M. A., & Adnan, T. (2020). Machine Learning in Accounting Research: A Computational Power to Wipe Out the Challenges of Big Data. *Asian Accounting and Auditing Advancement*, *11*(1), 55–70. https://4ajournal.com/article/view/79

Kafi, M. A., & Adnan, T. (2022). Empowering Organizations through IT and IoT in the Pursuit of Business Process Reengineering: The Scenario from the USA and Bangladesh. *Asian Business Review*, *12*(3), 67–80. https://doi.org/10.18034/abr.v12i3.658

Le, D. C., & Zincir-Heywood, A. N. (2019). Machine learning-based insider threat modeling and detection. In *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. IEEE. pp. 1-6.

Lika, R. A., Murugiah, D., Brohi, S. N., & Ramasamy, D. (2018). NotPetya: Cyber-attack prevention through awareness via gamification. In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 1-6). IEEE.

Mandapuram, M. (2016). Applications of Blockchain and Distributed Ledger Technology (DLT) in Commercial Settings. *Asian Accounting and Auditing Advancement*, *7*(1), 50–57. Retrieved from https://4ajournal.com/article/view/76

Mandapuram, M. (2017). Security Risk Analysis of the Internet of Things: An Early Cautionary Scan. *ABC Research Alert*, *5*(3), 49–55. https://doi.org/10.18034/ra.v5i3.650

Mandapuram, M., & Hosen, M. F. (2018). The Object-Oriented Database Management System versus the Relational Database Management System: A Comparison. *Global Disclosure of Economics and Business*, *7*(2), 89–96. https://doi.org/10.18034/gdeb.v7i2.657

Microsoft. (n.d.). *Security at Microsoft*. https://www.microsoft.com/en-us/professionalservices/security

National Institute of Standards and Technology. (2018). *Guide to Small and Medium Business Cybersecurity.* https://www.nist.gov/itl/smallbusinesscyber

Noever, D. (2019). Classifier suites for insider threat detection. *arXiv preprint arXiv:1901.10948*.

OWASP. (2021). *OWASP Top Ten Project*. Retrieved from https://owasp.org/Top10/

Ponemon Institute. (2020). Cost of a Data Breach Report. https://www.ponemon.org/

Pritam, N. (2020). Money makes the cyber-crime world go round - Verizon Business 2020 Data Breach Investigations Report. *Verizon.* https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report

Reddy, M., Bodepudi, A., Mandapuram, M., & Gutlapalli, S. S. (2020). Face Detection and Recognition Techniques through the Cloud Network: An Exploratory Study. *ABC Journal of Advanced Research*, *9*(2), 103–114. https://doi.org/10.18034/abcjar.v9i2.660

RED-GOAT. (2019). *Insider Threat Report.* Retrieved from https://red-goat.com/insider-threat-report-2019/

SANS Institute. (n.d.). *Security-Awareness.* https://sc.edu/about/offices_and_divisions/division_of_information_technology/security/docs/security-awareness-brochure.pdf

Simkins, B. J., Parikh, A., & Isbell, M. (2020). Digital forensics in the accounting classroom: A case for expanding coverage and skills in cybersecurity education. *Journal of Forensic Accounting Research*, 5(1), 53-71.

Smith, J. (2017). The Equifax Data Breach: Lessons Learned for Financial Institutions. *Journal of Financial Security*, 42(3), 123–145.

Symantec. (n.d.). *Antivirus - Symantec Endpoint Protection (SEP).* https://www.alaska.edu/oit/services/software-downloads/licensed-software/antivirus/

US-CERT. (2018). *Alert (TA17-132A): Indicators Associated with WannaCry Ransomware.* https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware

US-CERT. (2020). *Advanced Persistent Threat Activity Exploiting Managed Service Providers.* https://www.cisa.gov/news-events/alerts/2018/10/03/advanced-persistent-threat-activity-exploiting-managed-service/

--0--